DigiCert® Enterprise PKI Platform: Windows Hello for Business のサポート

時代はパスワードレスへ

パスワードレス認証は今、アクセスポイントでのセキュリティ向上を図りつつ、ユーザーのサインイン体験を簡素化できる方法として注目を集めています。どんなに強力なパスワードであってもリプレイ攻撃やフィッシング攻撃の対象となり、サーバーへの侵入を受けてしまう可能性がある一方で、ユーザー側からすれば強力なパスワードは記憶しておくのが難しいという面もあります。さらに、アクセス要求のたびに認証を求めるゼロトラストのセキュリティモデルを採用する企業が増えるにつれて、アクセスセキュリティは、攻撃を防ぎ企業の労働力を有効活用するうえで、IT 部門にとってますます重要な課題となっています。パスワードレス認証を導入すれば、エンドユーザーはパスワードを生成したり記憶したりする必要がなくなり、今まで以上に安全な手法で ID を認証することができます。

> **89%**
>
> **の Web アプリケーション侵害は、盗難クレデンシャルの利用や総当たり攻撃といった何らかのクレデンシャル悪用に関連しています。**
>
> --Verizon 2021 Data Breach Investigation Report

Windows Hello for Business: 証明書信頼モデル

Windows Hello for Business（WHfB）は、Microsoft が提供しているパスワードレス認証ソリューションであり、生体認証や PIN コード認証による PC やモバイル端末での強力な認証（多要素認証）を用いてサインイン / ログインを認証します。

WHfB の証明書信頼モデルは、公開鍵基盤（PKI）を利用した電子証明書を使用し、認証局（CA）が発行した証明書を用いて、Active Directory（AD）に認証を行うものです。

鍵信頼モデルでは、鍵を用いて AD を認証するため、自己署名証明書が必要です。

WHfB が採用する主要な 2 つの信頼モデル、すなわち鍵信頼モデルと証明書信頼モデルのうち、以下のような状況の企業には、証明書信頼モデルが好まれる可能性があります。

- ユースケース : 証明書信頼モデルでは、Windows ログオンで WHfB 用証明書をスマートカード証明書と同じように使用できます。
- ID およびアクセステクノロジー : エンドユーザー証明書の発行と管理にすでに PKI を利用している企業は、Windows Hello for Business と組み合わせて PKI を活用することもできます。

DigiCert® Enterprise PKI Platform と Windows Hello For Business

DigiCert Enterprise PKI Platform は、WHfB 用証明書による信頼モデルをサポートしており、お客様がパスワードレス認証の取り組みに求める、以下のようなユースケースと利便性を提供します。

- 事前に設定された証明書テンプレートとそれに対応する申請方法によって、WHfB 用証明書の管理を**簡素化**。
- Windows ドメインに接続されたワークステーションおよびドメインコントローラに対して WHfB が要求するクライアント認証済み証明書を自動化されたワークフローとゼロタッチプロビジョニングすることで、オンボーディングを**加速化**。
- 他の企業ユースケースを管理するのと同じプラットフォームを使って WHfB 用デジタル証明書を管理することで利便性が**向上**。

WHfB への対応は、DigiCert Enterprise PKI Platform の数多くの機能のひとつであり、自動化されたワークフロー、事前に設定された証明書テンプレート、複数の申請方法、サードパーティとの統合機能に基づいて、電子証明書のプロビジョニングと管理を簡素化したうえで提供します。

つまり、Windows Hello for Business の管理者にとって、以下のような利点があります。

PKI Platform の機能	利点
事前に設定された WHfB 向け証明書テンプレート	WHfB ドメインコントローラ、申請エージェント、およびユーザー認証用に事前定義された証明書テンプレートにより、DigiCert Auto-Enrollment Server（クライアントレス）を介して、ユーザーとデバイスの迅速なオンボーディングを促進
ゼロタッチの証明書ライフサイクル管理	証明書の更新、再発行、有効期限処理、および再プロビジョニングの自動化により、ユーザーの生産性とセキュリティが向上
強力な鍵の保護とポリシーの適用	TPM（トラステッドプラットフォームモジュール）を使用した鍵の生成および保護のオプションを提供し、TPM を使用するためのポリシー適用を実現
WHfB のサードパーティシステムやアプリケーションとのシームレスな統合	連携サービスと分散サービスに対する REST API、SCEP、EST、および SAML をサポートすることで統合が容易に
WHfB およびその他の電子証明書の一元的な管理および運用	証明書のライフサイクル管理、追跡、監査ログ、レポートを 1 つのプラットフォーム上で実行することで、企業全体の証明書環境を可視化、管理
迅速なプラットフォーム導入	ソフトウェアベースおよび HSM ベースの認証局の迅速な導入とオンライン認証局作成を促進
柔軟性と拡張性の高い PKI プラットフォーム	実績のある拡張性により、クラウド、オンプレミス、ハイブリッドのモデルを含む複数の PKI プラットフォーム導入オプションをサポート
多言語対応	すべての Web インターフェース、管理コンソール、エンドユーザー申請 Web ページで多言語をサポート

技術要件

DigiCert® Enterprise PKI Platform:	• ドメイン接続された Windows Server* 上の PKI Platform 8 と Autoenrollment Server、または • ドメイン接続された Windows Server 上の Enterprise PKI Manager と Autoenrollment Server（2022 年第 1 四半期より提供予定）
Windows Server オペレーティングシステム（OS）:	2019、2016、または 2012
ディレクトリサービス :	Windows Active Directory（AD）*、Azure AD
シングルサインオンソリューション :	Microsoft Active Directory Federation Services（ADFS）
ID データ同期ソリューション :	Azure AD Connect
クライアントマシン OS:	Windows 10 以降

* コンポーネントは、サポート対象の同じ Windows Server OS 上で稼働している必要があります

詳細については、**https://www.digicert.com/jp/pki/enterprise-pki-manager** のお問い合わせフォームよりお問い合わせください。